

1 --11. A method for configuring a firewall (1) in a computer system (2)
 2 comprising objects (3), and resources (4), for establishing an access control policy
 3 for the objects (3), the method comprising grouping the objects (3) of the system into
 4 internal and external protection domains (5, 6), ensuring establishing a firewall (a) for
 5 protection of an internal domain (5) relative to an external domain (6), and applying
 6 to the firewall a rule for controlling access between a source resource (4) and a
 7 destination resource only if said source and destination resources belong to the
 8 same internal or external protection domain (5 or 6).

1 12. A method according to claim 11, further comprising determining the
 2 protection domain of the resources (4) by means of firewall network interfaces (10)
 3 through which communications pass in order to reach said resources.

1 13. A method according to claim 12, further comprising defining zones (8)
 2 comprising networks or subnetworks, associating the network interfaces (10) of
 3 firewalls to which said zones are connected with an internal or external domain,
 4 determining the incoming and outgoing network interfaces (10) of current traffic,
 5 analyzing whether said network interfaces are attached to an internal or external
 6 domain, and applying the rule for controlling access only if both network interfaces
 7 are attached to the same internal domain (5), and the resources belong to the same
 8 protection domain.

1 14. A method according to claim 11, characterized in that it composes
 2 groups of objects (3) for which the access control policy is identical and the rule for
 3 controlling access is applied between each of the resources of a source group and a
 4 destination group.

1 15. A method according to claim 12, characterized in that it composes
 2 groups of objects (3) for which the access control policy is identical and the rule for
 3 controlling access is applied between each of the resources of a source group and a
 4 destination group.

- 1
- 2
- 3
- 4

- 1
- 2
- 3
- 4
- 5

- 1
- 2
- 3
- 4
- 5

- 1
- 2
- 3
- 4
- 5

- 1
- 2
- 3
- 4
- 5

- 1
- 2
- 3

4 (5) or (6) when the scope of the rule is local, and applying the rule to all of the
5 resources in question when the scope of the rule is global.

1 22. A method according to claim 16, further comprising characterizing the
2 rule for controlling access with a local or global scope, applying the rule to the
3 resources in question only if said resources belong to the same protection domain
4 (5) or (6) when the scope of the rule is local, and applying the rule to all of the
5 resources in question when the scope of the rule is global.

1 23. A device for configuring a firewall (1) in a computer system (2)
2 comprising resources (4) including objects (3) having an access control policy and
3 an established central configuration machine (14) for grouping the objects (3) of the
4 system into internal (5) and external (6) protection domains, a firewall (1) ensuring
5 the protection of an internal domain (5) relative to an external domain (6), and means
6 for applying to the firewall in question a rule for controlling access between a source
7 resource (4) and a destination resource only if said source and destination resources
8 belong to the same protection domain (5) or (6).

1 24. A device according to claim 23, characterized in that it further
2 comprises a graphical interface (15) from which an administrator (7) can enter the
3 domains (5) and (6) and the access control rules.

1 25. A device according to claim 23, characterized in that the graphical
2 interface allows the administrator (7) to define a local or global scope for the access
3 control rule, and in that the machine (14) applies the rule to the resources in question
4 only if said resources belong to the same protection domain (5) or (6) when the
5 scope of the rule is local, and applies the rule to all of the resources in question
6 when the scope of the rule is global.

1 26. A device according to claim 24, characterized in that the graphical
2 interface allows the administrator (7) to define a local or global scope for the access
3 control rule, and in that the machine (14) applies the rule to the resources in question
4 only if said resources belong to the same protection domain (5) or (6) when the

6 when the scope of the rule is global.--

[illegible]